



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,663	03/23/2007	Hector Daniel Elbaum	1866-8624US	5028

7590  
Laurence B. Bond  
TRASKBRITT  
P.O. Box 2550  
Salt Lake City, UT 84110

EXAMINER
----------

ST CYR, DANIEL

ART UNIT	PAPER NUMBER
----------	--------------

2876

MAIL DATE	DELIVERY MODE
-----------	---------------

01/19/2011

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/580,663	<b>Applicant(s)</b> ELBAUM ET AL.	
	<b>Examiner</b> Daniel St.Cyr	<b>Art Unit</b> 2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 23 December 2010.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-8, 10-27, 29 and 30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 23, 24, 29 and 30 is/are allowed.
- 6) ☒ Claim(s) 1-8, 10-22, 25-27, 29 and 30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 May 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### **Continued Examination Under 37 CFR 1.114**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/23/10 has been entered.

### **Claim Rejections - 35 USC § 102**

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-8, 10-16, are rejected under 35 U.S.C. 102(e) as being anticipated by Linehan, US Patent No. 7,103,575.

Linehan teaches enabling use of smart cards by consumer devices for internet commerce comprising: a secure data entry device 200/205 connected to the public data network 210; and a gateway device 215 connected to the public data network and to a private data network used for transmitting messages between financial institutions 220; wherein the secure data entry device comprises means for the user to enter identifying information of a card issued by the financial institution (see col. 10, lines 27-30), means for the user to enter the user's Personal Identification Number ("PIN"), means for encrypting the identifying information and PIN for

Art Unit: 2876

secure transmission, and means for transmitting the encrypted identifying information and PIN in a secure manner via the data transmission output over the public data network to the gateway device (see col. 6, lines 50+); wherein the gateway device includes means for transmitting the identifying information to the card-issuing financial institution and for receiving an approval response from the card-issuing financial institution over the private data network; and whereby the approval response provides authentication of the identifying information by the card-issuing financial institution (see col. lines 8-16). (see fig. 2, col. 9, line 64 to col. 10, line 41).

Re claim, wherein the public data network is the Internet (see fig.2, item 210).

Re claim 3, wherein the secure data entry device is connected to the public data network via a personal computer 205 (see fig.2).

Re claim 4 wherein the private data network is an inter-bank network used for the transferal of electronic transaction data (data are communicate between the issuing bank and the acquiring bank, the EMV and the four party protocol formed an integrated system) (see col. 7, lines 8-16, fig. 1-2).

Re claim 5, wherein the private data network is provided via a dedicated network operated for the sole purpose of conducting electronic financial transactions (the network is for connecting consumers with issuing and acquiring banks to conduct financial transactions).

Re claim 6, wherein the private data network is a virtual private network operated for the purpose of conducting electronic financial transactions via a host of public data network (the consumer initiate the transactions via a public data network) (see fig. 1-2).

Art Unit: 2876

Re claim 7, wherein the secure data entry device further includes: a card reader 200 for reading relevant information stored on the user's card; and a keypad to enable the user to enter data into the system (see col. 10, lines 21-35).

Re claim 8, wherein the card reader is able to read an of ISO 7816 smart card (see col. 10, line 26) (international standard type of cards).

Re claim 10, wherein said identifying information includes one or more of: the Primary Account Number associated with the card; the expiry date of the card; and the user's Personal Identification Number associated with the card (at least the PIN is associated with the card, see col. 10, line 27).

Re claim 11, wherein the identifying information is transmitted using a standard transaction message format compliant to ISO 8583 (financial transaction card originated message, see col. 9, line 64 to col. 10, line 41).

Re claim 12, wherein the ISO 8583 message used is one of an "0200" financial presentment message, and or an "0104" authorization message (these codes are standard transaction codes for ISO 8583, card originated transactions).

Re claim 13, wherein the gateway device also includes means for transmitting the approval response to the secure data entry device (see col. 12, lines 12-20).

Re claim 14, wherein the secure data entry device further includes means for deriving from the approval response verifiable proof that the customer's identifying information has been authenticated by the card-issuing financial institution (the authentication data from the issuing bank is sent to the secure entry device for verification, see col. 12, lines 12-20).

Art Unit: 2876

Re claim 15, wherein said proof is an authentication data block, consisting of data computed in a secure manner from the approval sent from the card-issuing bank (see col. 12, lines 12-20).

Re claim 16, wherein the data block is a whole or truncated encryption of the approval message derived using an encryption key stored securely within the secure data entry device ( using application authentication cryptogram, see col. 8, lines 54+ and col. 12, lines 12-20).

Re claim 27, the limitations have been addressed above.

### **Claim Rejections - 35 USC § 103**

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 17-22 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan in view of Flitcroft et al, US Pub. 2003/0028481. The teachings of Linehan have been discussed above.

Although Linehan teaches dynamic data authentication wherein random card numbers are generated to create certificates for protecting the security of electronic messages, Linehan fails to disclose or fairly suggests that the gateway device further includes means to generate a replacement card number transmitted over the private network upon receipt of the approval response from the card-issuing institution for performing transactions.

Flitcroft et al disclose a credit card system and method comprising: a central processing station 102, be operated by the credit card provider, the station 102 receives and processes

Art Unit: 2876

remotely generated credit card transactions; the credit card transactions can originate from a merchant in the conventional manner, e.g., by swiping a credit card through a card swipe unit 106 or can originate from any remote electronic device 104 (e.g., a personal computer); the remote devices can interface with the central processing station 102 through any type of network, including any type of public or propriety networks, or some combination thereof. For instance, the personal computer 104 interfaces with the central processing station 102 via the Internet 112; the central processing station 102 itself may include a central processing unit 120, which interfaces with the remote units via network I/O unit 118; the central processing unit 120 has access to a database of credit card numbers 124, a subset 126 of which can be designated as being available for limited use (referred to as the "available range"), the database 122 stores the mapping between a customer's fixed master credit card number and any outstanding associated limited use credit (see par. 0069-0070).

In view of Flitcroft's teachings, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to modify the teachings of Linehan to include means for managing and generating replacement card numbers for processing customers' transactions. Such modification would enhance the system's security due to the fact the actual card number is seal from merchants and others by generating limited use card numbers for each transaction (i.e. single use, limited amount, etc.). For instance, if a single use number were compromised during a transaction, the account owner would not worry because the unauthorized individual will not be able to reuse the compromised number for fraudulent transactions). Therefore, it would have been an obvious extension as taught by Linehan.

Art Unit: 2876

Re claim 17, Linehan as modified by Flitcroft et al provide means to generate replacement numbers upon issuer's approval.

Re claim 18, since Linehan teaches the secure device entry connected to the public data network, Linehan as modified by Flitcroft et al also transmit the replacement number via the public data network (see fig. 2 of Linehan).

Re claim 19, Linehan as modified by Flitcroft et al teach a single use number (see par. 0070 of Flitcroft).

Re claim 20, Linehan as modified by Flitcroft et al teach multiple use number (i.e. time limit, limited amount) (see par.0070).

Re claim 21, Linehan as modified by Flitcroft et al show that the consumer transmits information from the secure entry device to the PC, then to the merchant, from the merchant to acquiring bank, to the issuing bank, from the issuing bank to the gateway or the merchant information is transmitted from public data network to the gateway (see fig. 2, and 5).

Re claim 22, Linehan as modified by Flitcroft et al transmit identifying information (i.e. merchant information) in order to properly process the payment.

Re claim 25, Linehan as modified by Flitcroft et al include means for receiving payment transaction message from private network, modifying said message, transmitting said message to the issuer; whereby the gateway device is able to substitute actual card number for replacement number before transmitting the transaction message to the issuer (see figs. 2, 5 of Linehan and par. 0069-0070 of Flitcroft).

#### **Allowable Subject Matter**

6. Claims 23-24 and 28-29 are allowed over the prior art.



Art Unit: 2876

7. The following is a statement of reasons for the indication of allowable subject matter:

Although the prior art of record teaches a system and method for authenticating consumers which includes a private entry device communicating via a public data network to merchants and to the gateway, wherein the gateway provides virtual limited use card numbers replacing the actual card numbers and communicates to issuing institutions via a private data network, the prior art of record fails to disclose or fairly suggests that the bank identification number of the replacement card number is selected such that the payment transaction is routed through the gateway device on the private data network before being sent to the card-issuing institution or is directed over the private data to the gateway device by identifying the gateway device as a card-issuing institution of the replacement card number. These limitations in conjunction with other limitation in the claims were not shown by, would not be obvious over, nor would have been fairly suggested by the prior art of record.

#### **Response to Arguments**

8. Applicant's arguments with respect to claims 1-8, 10-27, and 29-30 have been considered but are moot in view of the new ground(s) of rejection.

#### **Additional remarks:**

In response to the applicant's argument regarding using a PIN pad, card reader, and encryption, the new prior art (7,103,575) teaches using a secured PIN pad, a card reader, and encrypting the financial information before transmitting the information via the public data network (see col. 10, lines 21-41 and col. 14, line 34-51).

In response to the applicant's argument that there is no secure data entry device that comprises a discrete device, the examiner respectfully disagrees. The prior art teaches using PIN

Art Unit: 2876

pad and card reader, these devices are considered discrete devices. Furthermore, with respect to the general arguments of the claims, see the rejection above.

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel St.Cyr whose telephone number is 571-272-2407. The examiner can normally be reached on Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DS

January 18, 2011

/Daniel St.Cyr/

Primary Examiner, Art Unit 2876